Relatório de Segurança

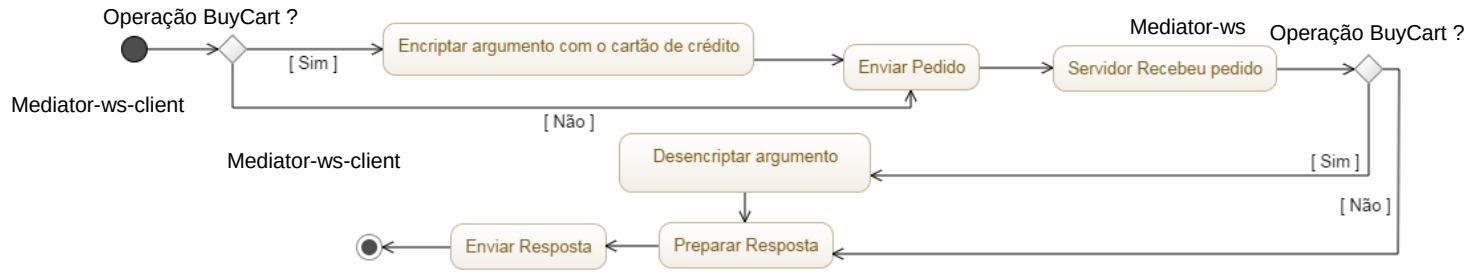
Grupo T59

http://www.github.com/tecnico-distsys/T59-Komparator

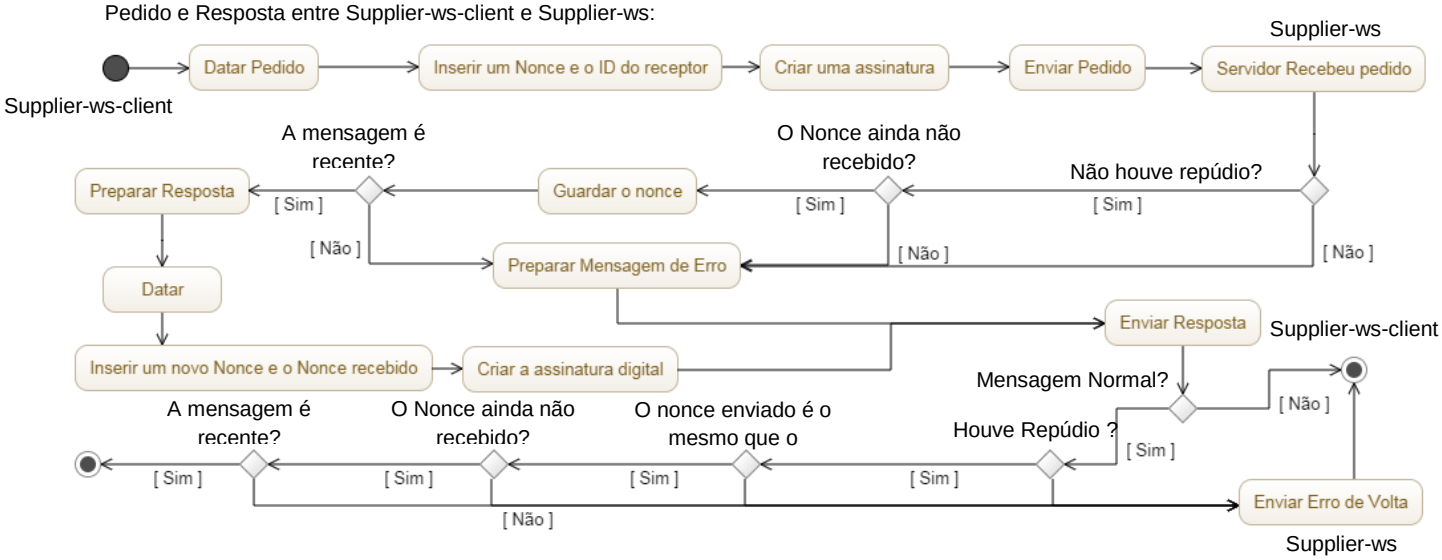
Ricardo Filipe
84621

Tiago Da Silva Letra
84627

Pedido e Resposta entre Mediator-ws-client e Mediator-ws:



Pedido e Resposta entre Supplier-ws-client e Supplier-ws:



No projeto existem 2 canais, um deles é entre o mediator e mediator client e outro entre o supplier e o supplier client.

No caso dos pedidos e respostas entre o mediator e mediator client foram usados 2 handlers um para o client e outro para o servidor. No caso do cliente, o handler verifica se a operação do pedido é o Buy Cart se for encripta o argumento do cartão de crédito com a chave pública do servidor. O handler do servidor verifica se o pedido recebido do cliente é uma operação BuyCart , desencripta o argumento do número do cartão de crédito, assim criando confidencialidade visto que só a entidade que encriptou e a que desencriptou podem saber o número. A mensagem SOAP na resposta mantém inalterada, mas no pedido só se mantem inalterado caso não seja uma o pedido não seja uma operação BuyCart.

Entre supplier e o supplier client são usados 5 handlers diferentes, 3 em cada. Antes de um pedido ser enviado para o supplier, é adicionado no cabeçalho do SOAP a data e a hora de quando a mesagem foi escrita(DateHandler), um número único gerado para o pedido encriptado com a chave publica do Supplier (NonceReceiverHandler), o id do Supplier (NonceReceiverHandler), e a assinatura digital(SignatureHandler). A mensagem fica da seguinte forma:

<soap:Envelope>...
<soap:Header>
<Data>Thu Jan 10 02:00:00 WEST 2017</Data>
<Nonces>(número encriptado)</Nonces>
<Id>T59_Supplier1</Id>
<Assinatura>(assinatura)</Assinatura>
</soap:Header>
<soap:Body>...</soap:Body>
</soap:Envelope>

Quando o Supplier recebe o pedido, os handler verificam a validade do cabelalho, primeiro verificam se documento não foi alterado através da assinatura, depois se nonce ainda não foi recebido por um pedido recente e por fim verifica se a mensagem foi enviado à menos de 3 segundos .Estes últimos dois handlers permitem validar a frescura e o primeiro verificar se não houve repúdio no pedido. Na resposta é adicionado ao cabeçalho da mensagem SOAP de novo a data pelo handler DateHandler, o nonce recebido no pedido, um novo número único gerado pelo Supplier ambos inseridos pelo NonceReceiverHandler e por fim a assinatura pelo handler SignatureSupplierHandler. Tanto o nonce gerado no supplier como o recebido no pedido são encriptados pela chave publica do mediador na resposta. A mensagem SOAP é representada da seguinte maneira:
<soap:Envelope>...
<soap:Header>
<Data>Thu Jan 10 02:00:01 WEST 2017</Data>
<Nonces>(número encriptado)</Nonces>
<Noncer>(número encriptado)</</Noncer>
<Assinatura>(assinatura)</gAssinatura>
</soap:Header>
<soap:Body>...</soap:Body>
</soap:Envelope>

Os handlers do cliente ao receberem a resposta, verificam se houve repúdio através da assinatura , de seguida verificam se o nonce enviado no pedido é igual ao enviado pelo servidor, isto permite autenticar o supplier porque só ele é que desencriptar o nonce e saber que número é, também verificado se o nonce gerado pelo supplier não foi recebido noutra resposta recente, no final validar a data em que mensagem foi enviada estas 2 últimas operações permitem validar a frescura da mensagem.

A razão porque é usado o nonce para verificar a frescura e não só a data é porque se só for usada a data um atacante pode repetir a mesma mensagem durante 3 segundos (período de tempo em que a mensagem é aceite pelo DateHandler), com o nonce isto já não acontece, pois só são aceites mensagem com menos de 3 segundos e tenham um nonce único.

Caso não seja possível fazer a autenticação, não haja frescura ou houve repúdio é criada uma mensagem de erro.